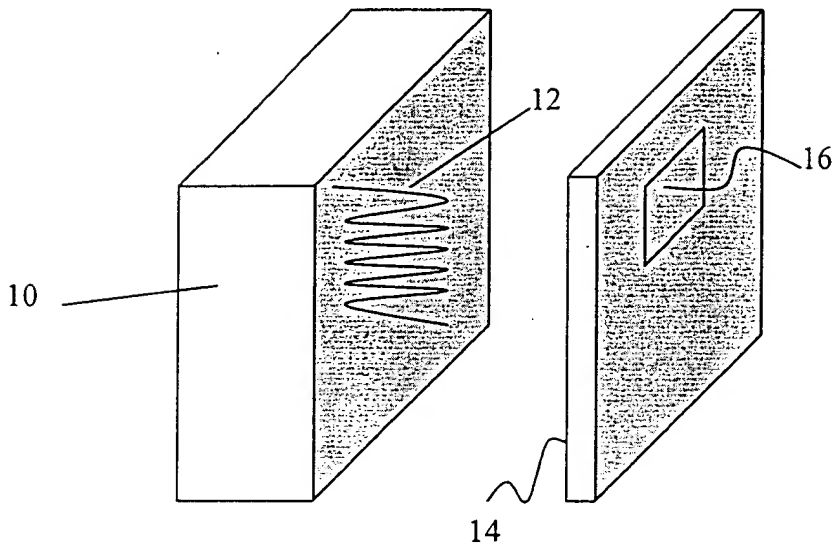

Figure 1

Smartcard Action	Transmission	Terminal Action
		Generate unique purchase ID and create transaction message
	← Purchase ID, TA 220 bits [TIU ID, Y_T] CA 355 bits	
Verify Certificate signed by CA 15,500 clock cycles Generate Random Number (R2) and sign transaction number using terminal's public key 15,500 clock cycles		
Send signed transaction data, hash and certificate signed by CA	→ [r1,s1] card 375 bits Hash 128 bits [Smartcard ID, Smartcard Public Key] CA 355 bits	
	←	Verify Certificate signed by CA Given the hash h and s1, deduce α^{kT} session key Recover message from r1
	R2 100 bits	Send R2 contained in message to card to prove identity and to acknowledge the provision of service
Check R2 to complete transaction		
Total computation time = 31,000 clock cycles	Total bits transmitted = 1533	

Figure 2